



2025 ACH Rule Amendments Summary

We want to ensure that as an ACH customer, you are informed of updates related to your responsibilities under the Nacha Operating Rules (i.e. “Rules”). This ACH Annual Letter is intended to highlight key Operating Rules and Responsibilities; it is not an inclusive list and not intended to be a replacement or substitution for the Rules, which are subject to change. We encourage you to consult Article Two of the Nacha Operating Rules for Originator obligations and Article Eight for definitions of terms used. To ensure continued compliance, all ACH Originators are required to have access to a current copy of the Rules. The ACH Rules for Corporate Originators is published annually. To request a copy, call Nacha at 1-800-487-9180 or visit the Nacha website at [eStore home | Nacha](https://www.nacha.org/eStore/home) . Copies can also be purchased from Wespay at <https://www.mywespay.org/public/s/information-center/store>.

Upcoming Nacha Originator Rule Changes

All Originators, Third-Party Senders and Third-Party Service Providers are required to comply with the Nacha Rules and any changes.

1. Origination Fraud Monitoring

Phase 1 – Effective March 20, 2026, for all ODFIs, Originators, Third-Party Service Providers, and Third-Party Senders with ACH volume greater than 6 million in 2023

Phase 2 – Effective June 19, 2026, this will apply to all ODFIs, Originators, Third-Party Services Providers, and Third-Party Senders

Summary

This rule will require all parties on the origination side of entries to have risk-based processes to identify fraudulently originated ACH entries.

Details

The Rules do not currently require Originators to have fraud monitoring processes, except for WEB debit entries. This rule will have requirements for all entries with the goal of detecting and preventing fraud from scams such as business email compromise and fake invoices.

Impact

Originators may already have processes such as anomaly detection or other “flags” that detect and prevent fraudulent entries. Each organization will need to review its processes and procedures to determine whether it needs to make updates to meet these new requirements.

2. RDFI Fraud Monitoring

Phase 1 – Effective March 20, 2026, for all RDFIs with ACH receipt volume greater than 10 million in 2023

Phase 2 – Effective June 19, 2026, for all RDFIs

Summary

This rule will require RDFIs to have processes to review received credit entries to identify potential fraud.

Details

The Rules will not prescribe how RDFIs review entries and will not require RDFIs to review each entry; each RDFI will determine how to comply with this requirement based on its environment.

Originator and Third-Party Sender Impact

This rule, along with the additional exception for funds availability and use of the R17 return reason code, will likely result in more returns of fraudulent entries, reducing losses for Originators, Third-Party Senders, and ODFIs.

3. Company Entry Descriptions

March 20, 2026

Summary

The Rules will require specific company entry descriptions for payroll entries and online purchases of goods.

Details

Originators will be required to use the description "PAYROLL" for PPD credits to pay wages, salaries, and other compensation.

Originators will be required to use the description "PURCHASE" for e-commerce purchases, which will be defined as "a debit Entry authorized by a consumer Receiver for the online purchase of goods"

Originator and Third-Party Sender Impact

Originators will need to review the company entry descriptions they use in ACH files and ensure they update these descriptions as required by the Rules. These standardized descriptions will help improve processes to monitor entries for potential fraud. Originators can begin using this description anytime but must comply with the requirements by the implementation date.

Fraud Trends and Prevention

Fraud schemes and attacks pose a serious threat to your business and customers. Fraud volumes continue to grow year over year, with electronic payment methods becoming increasingly vulnerable. Scams such as fake invoices, business or government impersonation, tech support, and fake checks continue to grow, as perpetrators relentlessly target businesses.

The Federal Trade Commission (FTC) has a resource page for businesses with details on industry scams and tools to help keep your employees and customers updated and help protect themselves.

As your financial partner, we want to help you avoid experiencing financial loss due to fraud. Contact us today at 866-563-1010 or via Chat within Commercial Online Banking to discuss what fraud prevention tools we offer that may be most beneficial to your business.

If you have any questions about these updates, please call us at 866-563-1010.

Thank you for choosing Umpqua Bank.